



(19) BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

Offenlegungsschrift

DE 195 11 298 A 1

(51) Int. Cl.⁶:
H 04 N 7/16
H 04 L 9/32
H 04 H 1/00
H 04 K 1/02

(21) Aktenzeichen: 195 11 298.9
(22) Anmeldetag: 28. 3. 95
(43) Offenlegungstag: 2. 10. 96

DE 195 11 298 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Schwenk, Jörg, Dr.rer.nat., 64846 Groß-Zimmern, DE

(56) Für die Beurteilung der Patentfähigkeit
in Betracht zu ziehende Druckschriften:

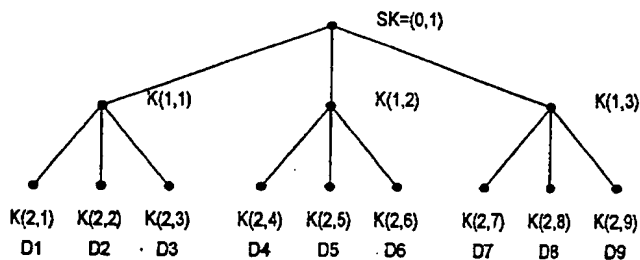
DE 38 27 172 C2
DE 38 02 612 C1
DE 37 17 022 A1
DE 35 24 472 A1
DE 33 25 858 A1
FR 28 96 567
US 52 31 666
US 52 02 921
US 48 81 264
US 46 61 658
US 43 09 569
EP 02 87 720 B1

EP 01 32 401 A2
JP 6-2 74 398 A
JP 5-3 27 748 A
JP 2- 88 859 A

SANTOSH, CHOKHANI: Toward a National Public
Key Infrastructure. In: IEEE Communications
Magazine, Sept. 1994, S.70-74;

(54) Verfahren zur Erteilung und zum Entzug der Berechtigung zum Empfang von Rundfunksendungen und Decoder

(57) Bei einem Verfahren und bei einem Decoder zur Erteilung und zum Entzug der Berechtigung zum Empfang von Rundfunksendungen, die durch Verschlüsselung geschützt sind, ist vorgesehen, daß die Schlüssel aller betroffenen Decoder eine Baumstruktur bilden, deren Wurzel ein Systemschlüssel zugeordnet ist, der zur Entschlüsselung eines mit der jeweiligen Rundfunksendung empfangenen Kontrollwortes dient, daß den der Wurzel und den einzelnen Knoten nachfolgenden Knoten Schlüssel zugeordnet sind, daß den Blättern dieses Baumes feste Schlüssel zugeordnet sind, die eindeutig einem Decoder oder einem Teil eines Decoders (z. B. einer Chipkarte) zugeordnet sind, daß die Schlüssel, die jeweils einen Ast der Baumstruktur bilden, in jeweils einem Decoder gespeichert werden und daß die in jeweils einem Decoder gespeicherten Schlüssel zur Entschlüsselung von empfangenen Kryptogrammen dienen, welche Änderungen der gespeicherten Schlüssel und des gespeicherten Systemschlüssels bewirken, daß diejenigen Schlüssel, die solchen Knoten zugeordnet sind, welche einem bestimmten Knoten unmittelbar nachfolgen, dazu dienen, Kryptogramme zu entschlüsseln, die einen Schlüssel enthalten, der dem bestimmten Knoten neu zugeordnet werden soll.



DE 195 11 298 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 08.98 602 040/175

5/27

BEST AVAILABLE COPY

Die Erfindung betrifft ein Verfahren zur Erteilung und zum Entzug der Berechtigung zum Empfang von Rundfunksendungen, die durch Verschlüsselung geschützt sind, mit einem Decoder und einen zur Durchführung des Verfahrens geeigneten Decoder.

Gebührenpflichtige Rundfunksendungen, die auch unter den Stichworten Pay-TV, Pay-Radio, bekanntgeworden sind, werden mit einem Schlüssel CW verschlüsselt. Benutzer werden dadurch zum Empfang berechtigt, daß man ihnen den Schlüssel (Kontrollwort) CW vertraulich zukommenläßt. Dazu wird im allgemeinen dem Benutzer ein persönlicher Schlüssel PK zur Verfügung gestellt, der meist physikalisch gegen Vervielfältigung gesichert, beispielsweise auf einer Chip-Karte gespeichert ist.

Das Kontrollwort CW wird verschlüsselt als Kryptogramm ECM (Entitlement Control Message) über einen Datenkanal des Rundfunksenders vom Empfänger bzw. Decoder empfangen. Durch Entschlüsselung dieses Kryptogramms mit Hilfe des persönlichen Schlüssels PK wird das Kontrollwort CW wiedergewonnen. Bei dem unter dem Namen EuroCrypt bekanntgewordenen System wird ein weiteres Kryptogramm EMM (Entitlement Management Message) eines Schlüssels SK gesendet. Dieses Kryptogramm kann mit Hilfe von PK entschlüsselt werden. Der so erhaltene Schlüssel SK dient zur Berechnung von CW aus dem Kryptogramm ECM. Dieses Zugangskontrollsystem ist in DIN EN 50094 beschrieben. Sicherheitshalber wird der Schlüssel CW häufig gewechselt.

Eine wichtige Aufgabe des Zugangskontrollsystems besteht darin, Benutzern, die ihre Gebühren nicht bezahlt haben, die Berechtigung zum Empfang der Rundfunksendung zu entziehen. Dieses kann einerseits durch eine negative Adressierung geschehen, bei welchem an den Decoder eine Nachricht geschickt wird, in welcher dieser aufgefordert wird, seine Tätigkeit einzustellen. Diese Möglichkeit ist jedoch grundsätzlich unsicher, da derartige Nachrichten von einem betrügerischen Benutzer abgefangen werden können und damit unwirksam sind.

Bei der positiven Adressierung wird eine Abschaltung des Decoders dadurch bewirkt, daß die in ihm enthaltene Information wertlos gemacht wird. Das geschieht dadurch, daß alle anderen Decoder neue Informationen erhalten, die zum Entschlüsseln zukünftiger Rundfunksendungen unbedingt gebraucht werden, nur der abzuschaltende Decoder nicht.

Das Verfahren der positiven Adressierung führt zwar mit Sicherheit zur Abschaltung des Decoders des jeweiligen Benutzers, es ist allerdings mit großem Aufwand verbunden, da zum Abschalten eines Decoders Nachrichten an alle anderen Decoder gesendet werden müssen.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Erteilung und zum Entzug der Berechtigung zum Empfang von Rundfunksendungen vorzuschlagen, bei welchem die zur Entschlüsselung erforderlichen Informationen in einem bestimmten Decoder wertlos gemacht werden können, ohne daß alle anderen Decoder einzeln adressiert werden müssen.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst,

— daß die Schlüssel aller betroffenen Decoder eine Baumstruktur bilden, deren Wurzel ein Systemschlüssel zugeordnet ist, der zur Entschlüsselung

eines mit der jeweiligen Rundfunksendung empfangenen Kontrollworts dient,

- daß den der Wurzel und den einzelnen Knoten nachfolgenden Knoten Schlüssel zugeordnet sind,
- daß den Blättern dieses Baumes feste Schlüssel zugeordnet sind, die eindeutig einem Decoder oder einem Teil eines Decoders (z. B. einer Chipkarte) zugeordnet sind,
- daß die Schlüssel, die jeweils einen Ast der Baumstruktur bilden, in jeweils einem Decoder gespeichert werden und
- daß die in jeweils einem Decoder gespeicherten Schlüssel zur Entschlüsselung von empfangenen Kryptogrammen dienen, welche Änderungen der gespeicherten Schlüssel und des gespeicherten Systemsschlüssels bewirken,
- daß diejenigen Schlüssel, die solchen Knoten zugeordnet sind, welche einem bestimmten Knoten unmittelbar nachfolgen, dazu dienen, Kryptogramme zu entschlüsseln, die einen Schlüssel enthalten, der dem bestimmten Knoten neu zugeordnet werden soll.

Bei 1.000.000 Decodern müßten bei dem bekannten Verfahren 999.999 Nachrichten übertragen werden, um einen der Decoder zu deaktivieren. Bei dem erfindungsgemäßen Verfahren mit beispielsweise einem 2-ären Baum der Tiefe 20 sind etwa nur 40 Nachrichten notwendig.

Zur Verschlüsselung der Daten können bei dem erfindungsgemäßen Verfahren sowohl symmetrische als auch asymmetrische Verfahren angewendet werden.

Eine vorteilhafte Ausführungsform des erfindungsgemäßen Verfahrens besteht darin, daß die Baumstruktur m -regulär ist, wobei $m^t \geq n$ gilt mit m = Zahl der einem Knoten oder der Wurzel nachfolgenden Knoten, t = Zahl der von Knoten gebildeten Ebenen und n = Zahl der Decoder. Dadurch ist eine einfache Zuordnung der Kryptogramme, welche Änderungen der gespeicherten Schlüssel bewirken, möglich.

Zum Entzug der Berechtigung eines bestimmten Decoders kann bei dem erfindungsgemäßen Verfahren vorgesehen sein, daß

- für jeden Decoder außer dem bestimmten Decoder, der zusammen mit dem bestimmten Decoder demselben Knoten nachfolgt, ein Kryptogramm gesendet wird das den mit dem festen Schlüssel des Decoders verschlüsselten Schlüssel enthält, der dem gemeinsamen Knoten neu zugeordnet wird,
- beginnend mit dem Knoten, der dem gemeinsamen Knoten vorausgeht, bis zur Wurzel für jeweils alle nachfolgenden Knoten aller dem bestimmten Decoder mittelbar vorausgehenden Knoten jeweils ein Kryptogramm gesendet wird, das den mit dem Schlüssel des jeweils nachfolgenden Knotens verschlüsselten Schlüssel enthält, der dem dem bestimmten Decoder mittelbar vorausgehenden Knoten neu zugeordnet wird.

Ein vorteilhafter Decoder zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche ist dadurch gekennzeichnet, daß mehrere Schlüssel speicherbar sind, wobei mindestens ein Teil der Schlüssel durch mit den Rundfunksendungen empfangene Kryptogramme, die mit Hilfe eines der gespeicherten Schlüssel entschlüsselbar sind, veränderbar sind.

Ein Ausführungsbeispiel der Erfindung ist in der


Zeichnung anhand mehrerer ren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 eine schematische Darstellung der eine Baumstruktur bildenden Knoten, denen jeweils ein Schlüssel zugeordnet ist, wobei die Zahl der Decoder gegenüber der Wirklichkeit stark verringert ist, und

Fig. 2 eine Abfolge von auszusendenden Nachrichten zum Entzug der Berechtigung eines bestimmten Decoders.

Fig. 1 zeigt als Beispiel einen 3-ären Baum der Tiefe 2 mit Schlüsseln, welche den Knoten des Baums zugeordnet sind. Die Schlüssel $K(2,i)$ sind fest jeweils einem Decoder D_i bzw. einer Chipkarte zugeordnet. In dem dargestellten Beispiel gilt $i = 1, \dots, 9$. Der Wurzel des Baums ist der Systemschlüssel $SK = K(0,1)$ zugeordnet, während den m Nachfolgeknoten desjenigen Knoten, dem der Schlüssel $K(r,s)$ zugeordnet ist, die Schlüssel $K(r+1, m^{s-1}+1), \dots, K(r+1, m^{s-1}+m)$ zugeordnet sind.

Einem Decoder mit dem Schlüssel $K(m, x)$ — beim in Fig. 1 dargestellten Beispiel $K(2,i)$ — kann die Berechtigung, ein gebührenpflichtiges Rundfunkprogramm zu empfangen, dadurch erteilt werden, daß ihm gültige Schlüssel auf dem Weg innerhalb des Baums von $K(m,x)$ nach $K(0,1)$ mitgeteilt werden. Dazu sind maximal $t-1$ Nachrichten mit den Kryptogrammen der jeweils nächst höheren Schlüssel notwendig. Einem Decoder mit dem Schlüssel $K(m,x)$ kann die Berechtigung, ein gebührenpflichtiges Rundfunkprogramm zu empfangen, dadurch entzogen werden, daß man alle Schlüssel auf dem Weg von $K(m,x)$ nach $K(0,1)$ ersetzt. Dazu sind maximal $t \cdot m$ Nachrichten mit den Kryptogrammen der neuen Schlüssel erforderlich. Die Schlüssel, die zur Erteilung oder zum Entzug der Berechtigung ausgetauscht werden müssen, können bei Verwendung einer regulären Baumstruktur leicht berechnet werden.

Fig. 2 zeigt eine Folge von Nachrichten, um den Decoder D_9 mit Hilfe der in Fig. 1 beschriebenen Baumstruktur der Schlüssel zu deaktivieren. Jede Nachricht kann über einen Rundfunkkanal ausgestrahlt werden. Sie besitzt eine Adresse und eine Nutzlast, die in Fig. 2 durch einen senkrechten Strich getrennt sind. Mit Hilfe der Adresse erkennt jeder Decoder, ob eine bestimmte empfangene Nachricht von ihm verarbeitet werden muß. Die Nutzlast enthält ein Kryptogramm, das nur von den adressierten Decodern ausgewertet werden kann. Dabei bedeutet die Notation $A < B >$, daß die Information B mit dem Schlüssel A verschlüsselt wurde. Der Algorithmus zur Entschlüsselung ist im Decoder bekannt.

Zeile a der Fig. 2 zeigt eine Nachricht an den Decoder D_7 , mit welchem dieser einen neuen Schlüssel $K(1,3)$ neu erhält. Der Decoder D_8 erhält ebenfalls den gleichen neuen Schlüssel, der jedoch in diesem Fall über den Schlüssel $K(2,8)$ entschlüsselt wird (Zeile b). In der Nachricht gemäß Zeile c wird eine Adresse angegeben, die den Decodern D_1 bis D_3 gemeinsam ist und in Fig. 2 mit Gruppe 1 bezeichnet ist. Diese haben gemeinsam den Schlüssel $K(1,1)$, der zur Entschlüsselung des neuen Systemschlüssels SK_{neu} dient. In gleicher Weise wird dann für die Gruppe 2 (Decoder D_4 bis D_6) und für die Gruppe 3 (Decoder D_7 bis D_9) der neue Systemschlüssel SK_{neu} übertragen (Zeilen d und e). Dabei ist allerdings der Decoder D_9 nicht in der Lage, das Kryptogramm $K(1,3)$ neu $< SK_{\text{neu}} >$ zu entschlüsseln. Der Decoder D_9 erhält somit keine neuen Systemschlüssel SK_{neu} und kann die darauf folgend übertragenen Nutz-

signale nicht mehr decodieren.

Patentansprüche

1. Verfahren zur Erteilung und zum Entzug der Berechtigung zum Empfang von Rundfunksendungen, die durch Verschlüsselung geschützt sind, mit einem Decoder, **dadurch gekennzeichnet**,

— daß die Schlüssel aller betroffenen Decoder eine Baumstruktur bilden, deren Wurzel ein Systemschlüssel zugeordnet ist, der zur Entschlüsselung eines mit der jeweiligen Rundfunksendung empfangenen Kontrollwortes dient,

— daß den der Wurzel und den einzelnen Knoten nachfolgenden Knoten Schlüssel zugeordnet sind,

— daß den Blättern dieses Baumes feste Schlüssel zugeordnet sind, die eindeutig einem Decoder oder einem Teil eines Decoders (z. B. einer Chipkarte) zugeordnet sind,

— daß die Schlüssel, die jeweils einen Ast der Baumstruktur bilden, in jeweils einem Decoder gespeichert werden und

— daß die in jeweils einem Decoder gespeicherten Schlüssel zur Entschlüsselung von empfangenen Kryptogrammen dienen, welche Änderungen der gespeicherten Schlüssel und des gespeicherten Systemschlüssels bewirken,

— daß diejenigen Schlüssel, die solchen Knoten zugeordnet sind, welche einem bestimmten Knoten unmittelbar nachfolgen, dazu dienen, Kryptogramme zu entschlüsseln, die einen Schlüssel enthalten, der dem bestimmten Knoten neu zugeordnet werden soll.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß die Baumstruktur m -regulär ist, wobei in $m^t \geq n$ gilt mit m = Zahl der einem Knoten oder der Wurzel nachfolgenden Knoten, t = Zahl der von Knoten gebildeten Ebenen und n = Zahl der Decoder.

3. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet**, daß zum Entzug der Berechtigung eines bestimmten Decoders

— für jeden Decoder außer dem bestimmten Decoder, der zusammen mit dem bestimmten Decoder demselben Knoten nachfolgt, ein Kryptogramm gesendet wird, das den mit dem festen Schlüssel des Decoders verschlüsselten Schlüssel enthält, der dem gemeinsamen Knoten neu zugeordnet wird,

— beginnend mit dem Knoten, der dem gemeinsamen Knoten vorausgeht, bis zur Wurzel für jeweils alle nachfolgenden Knoten aller dem bestimmten Decoder mittelbar vorausgehenden Knoten jeweils ein Kryptogramm gesendet wird, das den mit dem Schlüssel des jeweils nachfolgenden Knotens verschlüsselten Schlüssel enthält, der dem dem bestimmten Decoder mittelbar vorausgehenden Knoten neu zugeordnet wird.

4. Decoder zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß mehrere Schlüssel speicherbar sind, wobei mindestens ein Teil der Schlüssel durch mit den Rundfunksendungen empfangene Krypto-

gramme, die mit Hilfe eines der gespeicherten
Schlüssel entschlüsselbar sind, veränderbar sind.

Hierzu 1 Seite(n) Zeichnungen

5

10

15

20

25

30

35

40

45

50

55

60

65

- Leerseite -

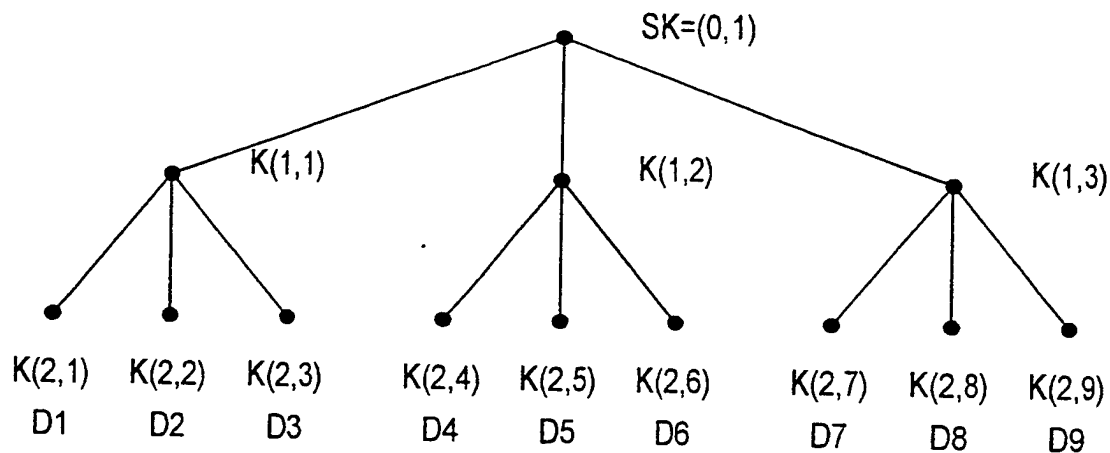


Fig.1

a	D7		$K(2,7) < K(1,3)_{\text{neu}} >$
b	D8		$K(2,8) < K(1,3)_{\text{neu}} >$
c	Gruppe1		$K(1,1) < SK_{\text{neu}} >$
d	Gruppe2		$K(1,2) < SK_{\text{neu}} >$
e	Gruppe3		$K(1,3)_{\text{neu}} < SK_{\text{neu}} >$

Fig.2